"CYBER WARRIOR": INFORMATION SUPERIORITY THROUGH ADVANCED MULTI-SENSORY COMMAND AND CONTROL TECHNOLOGIES

GILBERT G. KUPERMAN[1]
RANDALL D. WHITAKER, Ph.D.[2]
CAPT SCOTT M. BROWN, Ph.D.[1]

[1] Air Force Research Laboratory, AFRL/HECA, WPAFB, Ohio 45433, USA
[2] Logicon Technical Services Inc., P.O. Box 317258, Dayton, Ohio, 45431, USA

Abstract. This paper explores the functions of a conceptual, future "watch center" whose mission is to support Air Force information assurance requirements. A cognitive systems engineering approach is described through the insertion of multi-sensory, user interface technologies may be accomplished.

Key Words: Information Warfare, Command and Control, Human System Interface, Cognitive Systems Engineering

1. INTRODUCTION

The United States Department of Defense (DoD) is reducing the number of its personnel. As a result, there is a need for amplifying operational efficiency and effectiveness for remaining warfighters. At the same time, DoD is modernizing its capabilities to meet a diverse spectrum of anticipated missions. These challenges are outlined in Joint Vision (JV) 2010 (Shalikashvili; 1996)—"… the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."

Among the emerging warfighting demands, JV2010 emphasizes the importance of information superiority—"the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Achieving and maintaining information superiority will require both offensive and defensive information operations (IO). Years of United States Air Force (USAF) analysis and doctrinal development (e.g., Widnall and Fogleman, 1996) have identified some key requirements for achieving information superiority, and USAF efforts now concentrate on achieving three tasks:

- generating an overall information operations concept of operations (CONOPS)
- designating information operations command and control centers at the MAJCOM (major command) and Service levels
- equipping these centers to handle information operations performance demands

The USAF Information Warfare CONOPS (December 1999) addresses the first of these tasks. Effort on the second task has resulted in various information operations centers being identified (e.g., USSPACECOM's Joint Task Force-Computer Network Defense, MAJCOM network operations and security centers, numbered air forces' Information Warfare Flights). This article addresses the third required task by outlining the key research topics and introducing our research program ("Cyber Warrior") to develop advanced technologies enabling information operations staff to achieve information superiority.

2. THE WATCH CENTER AND ITS FUNCTIONS

These advanced technologies are discussed in the context of a prospective information operations "watch center" providing the Air Force battlespace management capability in overseeing and conducting defensive information warfare (DIW) operations such as (e.g.) attack assessment and response management. Lower echelon centers will report to this center, which will coordinate with its counterparts in the other Services and report upward to one or more DoD-level centers.

The watch center's central position in the USAF IO infrastructure makes it the primary USAF clearinghouse for IO data reachback. Other USAF operational units will be able to reachback to the watch center to learn of current and projected system status and posture, as well as to maintain situational awareness on relevant events. In addition, this reachback capability is required for the watch center's own operations. Owing to the watch center's responsibility for global Air Force information operations, its personnel may be detailed anywhere in the world supporting USAF theater missions. Because these "forward deployed" staff will need to draw on watch center resources, the center must afford efficient reachback for its own staff in addition to other USAF units.

The watch center would perform its most critical functions during an information attack against Air Force information systems (Kuperman, 1998). Functional requirements can be subdivided into three categories based on the three phases of attack events (pre- / trans- / post-attack). The following sections provide an overview of watch center functions for each of these three phases.

***Pre-Attack Phase**:* This is the default or background context of continuous watch center operations. The watch center will monitor and report the current status and readiness of lower echelon systems and networks. The scope of protective monitoring will be established and maintained through link and node analyses of USAF information assets, prioritized with respect to the assessed mission criticality of the functions they perform. Intrusion detection sensors installed on USAF information systems will feed a constant stream of data captured and analyzed by intrusion detection, network mapping and monitoring tools. Any unusual patterns of activity will become the subject of alerts to (e.g.) system administrators. Intelligence and open sources of information indicating changes to threat posture and capabilities will be assessed as evidence for impending attacks. This assessment will employ threat knowledge bases documenting the capabilities and methods of potential sources of information attack.

***Trans-Attack Phas**e:* Identifying, characterizing, and assessing the objectives of emergent attacks will be a critical watch center function. Attacks may be isolated discrete events or sets of multiple events distributed over both time and space, perhaps combining multiple attack methods. Incident reports (IRs) from lower echelons will be received, correlated and assessed. If an attack event is recognized, the watch center will generate a best assessment of its nature, source, and objectives. Minimizing damage to or disruption of USAF information processing capabilities will be the primary criterion in response selection. Defensive responses appropriate to this criterion in the context of the assessed attack will be recommended and, depending on the rules of engagement, implemented.

***Post-Attack Phase**:* Managing the recovery and reconstitution processes would be the major post-attack function of the watch center. The direct effects of the attack would be mitigated, information-processing capabilities would be restored, and Air Force mission capabilities would be reestablished. The watch center would provide USAF-wide status information on attacked resources and update its threat (and other) knowledge bases to increase its ability to recognize subsequent operations.

The watch center functional characteristics outlined above all pertain to data and information processing. Watch center personnel will be making critical decisions under intense time pressures, relying all the while on the data and information at hand. As such, watch center operations entail a high degree of cognitive activity on the part of staff members. The implications of this cognitively intensive work are discussed in the next section.

3. COGNITIVE DEMANDS ON WATCH CENTER WARFIGHTERS

"Information warfare, in its essence, is about…the way humans think and, more important, the way humans make decisions." (Stein, 1996)

Effective information operations entail some of the most extreme warfighter demands ever encountered. This is especially true for information operations, where the prospects include the fastest, most numerous, most anonymous, and most rapidly reconstitutable attackers in military history. The information operations mission must be accomplished in an environment ("cyberspace") where "fog" is common and routine access can become pure "friction." Moreover, the operations tempo is marked in milliseconds, and this makes information operations the warfighting effort most reflective of Col. John Boyd's (1987) analysis in terms of adversaries' OODA (Observe-Orient-Decide-Act) Loops.

High performance information operations entail global situation awareness (SA), efficient threat identification, and effective attack assessment. To achieve these ends watch center staff must monitor, manage, and manipulate data streams and information artifacts large in number, high in complexity, and dynamic in the extreme. These activities, like the battlespace itself, are predicated on data, inference, and decision making. Information operations command and control is therefore a cognition-intensive mission—i.e., one whose requisite burdens fall mainly on the abilities of warfighters (individually and in teams) to perceive, characterize, evaluate, and decide responses to threats.

Our brief description of the watch center illustrates a number of areas in which the decision-maker's cognition is critical to operations. Moreover, these key areas each entail issues that remain open research topics. The following paragraphs offer an illustrative selection of cognition-critical areas and issues deriving from relevant research at AFRL/HEC and elsewhere.

Effective situational awareness must be obtained and maintained by a watch center staff that may be distributed all around the world. How effective situation awareness can be assured in this operational context remains an open issue. Bolstad and Endsley (1999) describe the problems associated with shared/distributed situational awareness and posit a research effort directed at their solution. Prior AFRL/HEC-sponsored analysis of the Air Intelligence Agency's Information Operations Center (Larsen, 1997) highlights factors impeding team situation awareness (e.g., loss of situational knowledge during shift changes). One key facilitator of distributed situation awareness—a common information space upon which all team members may focus—mandates watch center technologies configured to provide staff such a shared information asset.

Overall situational assessment will be conveyed by the information condition (INFOCON) level (Harreld, 1998), a progression of assessed threat states. This assessment, based on recognition and characterization of emerging information attacks, will be particularly challenging since attacks may well exhibit multiplicity of time, source, technique, and target. This challenge is amplified by the fact that understanding the motivations and methods of cyber-attackers is itself a new topic of research (McCloskey and Stanard, 1999).

The pre- and trans-attack phases of watch center operations will require constant vigilance (Grossman, 1999) over information networks watching for perturbations indicative of attack conditions. The importance of even relatively small deviations from normalcy may take on greater weight as the information condition (INFOCON) escalates.

Previous decision making studies within the DoD have highlighted some of the issues that must be addressed. For example, MacMillan *et al.* (1998) note that "decision makers may lack the subtle vigilance required to detect small deviations from a pattern, and can be lulled into a false sense of security if they have seen a similar pattern many times."

Response selection is a decision making task which will impose significant cognitive burden on watch center staff subject to extremely short response timeframes. This burden will be exacerbated by the need to deal with necessarily conflicting goals (Flach and Kuperman, 1998). For example, an obvious goal would be to minimize or mitigate damage to own-force information systems, which suggests taking an attacked system offline as soon as possible. This clashes with the goal of allowing the attack to continue so as to gather additional diagnostic data for the purposes of (e.g.) countermeasures selection and/or defensive adaptation.

More generally, decision making is a challenging research domain. In the subject context (defensive response selection) the watch officer is pitted against an adversary of potentially unknown capabilities and intent. Llinas, *et al.* (1998) explore adversarial decision making in the context of information warfare. Their analysis identifies the human-centered issue of trust in automated decision support aids as critical in achieving a robust and acceptable balance in automated versus operator-performed functional allocation. More generally, research in naturalistic decision making (Klein, 1997; Klein *et al.*, 1989; Kuperman, 2000) can be leveraged to configure technologies to provide watch center staff with critical cues facilitating fast-paced decision processes. Moreover, such efforts can lead to more effective specifications for training watch center staff (Pliske *et al.*, 1997)—an important payoff in light of DoD personnel reductions.

Watch center warfighters will need information technologies that facilitate their grappling with the cognitive demands of the IO mission. This in turn requires that such technologies been specified with respect to the warfighters' informational requirements. The next section will provide a summary review of watch center informational requirements as they relate to specific aspects of information operations. After this review, we shall introduce and discuss our advanced development project ("Cyber Warrior"), which is planned to meet these information requirements via technologies developed for USAF IO watch centers.

4. A REVIEW: WATCH CENTER INFORMATION REQUIREMENTS

Cognition entails information processing. Cognitive demands are imposed in proportion to the mass of information with which warfighters must process, and these demands are alleviated to the extent this informational mass is reduced to only that optimum amount necessary to accomplish a given decision making task. In this section, we shall review some of the key watch center information elements we have already identified as crucial research and development topics.

4.1 The 'Big Picture': A Summary View of the Battlespace

A central point of reference in Battle Management/Command, Control, Communications and Computers, Intelligence, Surveillance, and Reconnaissance is a shared or mutually accessible model of the domain in which operations are conducted. Historically, this model has been provided in the form of a geospatial map (e.g., a 2D cartographic product on a wall or a 3D model on a table). In information operations, the battlefield is that paradoxically non-spatial 'space' of objects and actions colloquially labeled 'cyberspace'. Modeling 'cyberspace' is considerably less straightforward than modeling 'geospace'. 'Geospace' provides for absolute location (i.e., one object in one place at one time). Such a fixed condition is relatively unknown in cyberspace, unless one prioritizes physical elements (i.e., computers; cables) as the main objects of interest. For the most part, 'cyberlocation' is a matter of changeable and relative coordinates (e.g., IP addresses, domain names, URLs).

What, then, would be the foundation of a useful map of cyberspace? In information operations, the minimal object of attack is a particular computing platform. This happens to be the constituent element comprising the maximal object of attack (the network). Our research testbed includes an interactive Datawall array -- a large display/manipulation surface developed at the Air Force Research Laboratory's Information Directorate. The Datawall, as a large display surface, affords us the capacity to present operators with relatively large and complex graphics. It is straightforward to conclude that a 'network map' depiction of own-force computer systems and their interconnections is a good default candidate for a battlespace map.

Such a map would be complex given the number of platforms. Furthermore, operators and analysts will probably need to 'zoom' in and out so as to address multiple ranges of network assets based on (e.g.) extent of attacks or disruption. The IP addressing scheme consists of a single composite numerical string subdivided into four segments. These four segments index network assets (i.e., computing platforms) down to the level of individual computers. This addressing architecture could be exploited as a simple 'zoom hierarchy', by allowing operators to select a representational scope equivalent to one or another of the segments.

Because the IP addressing architecture is a strict hierarchy, one should only need to index a higher level to address the entire set of IP addresses subsumed beneath that level. As a result, the IP architecture provides an organization amenable to 'drill-down' using a graphic representation of each level (top to bottom), with specific subsets being addressable via 'point and click'. As such, we are focusing upon IP addressing being employed as the default organizational principle for the main Datawall network map. This does not preclude other options. However, at this very early stage this option is attractive for its simplicity and universality of application.

4.2 'Slicing' the Big Picture: Different Perspectives on the Network Map

The provision of a network map on a display is helpful, but it is not a complete answer to IO watch center needs. It is not only the IP address and/or relative position in an interconnected network, which identify and differentiate the elements of interest (i.e., the computer platforms). The watch center operator may wish to exploit distinctions that qualify or characterize the general class of 'all devices with an IP address'. A (non-exhaustive) list of examples for such distinctions includes:

- Classification by hardware type
- Classification by operating system
- Classification on the grounds of one or more resident software packages
- Distinctions between 'attacked' and 'unattacked' nodes
- Distinctions among 'operational', 'questionable', and 'healthy' platforms
- Classification by type of attack
- Classification by severity of attack / damage
- Classification by function (in context of operations)

- Classification by ‘owner’ (in context of organizational units)
- Classification by military (warfighting or support) mission

It should be clear that the range of possible criteria for sorting and indexing platforms may prove arbitrarily large, as would the number of individual / specialized ‘maps’ necessary to provide each and every such criterion to the operator(s). It should be similarly clear that trying to provide a huge list of all possibly useful ‘maps’ would prove a cognitive burden on the user as well as a burden to the information technologies handling these materials. In addition, it is reasonable to suppose that circumstances may warrant combinations of distinctions (e.g., the set of all intellignce platforms subject to a specific type of attack)—a prospect which would radically increase the number of individual ‘maps’ necessary to address the range of potential situations.

What we need is a modular set of ‘overlays’ or ‘filters’ which could be freely combined atop a basic network map to afford operators the ability to rapidly ‘sort’ or ‘slice’ their object(s) of primary reference in accordance with their immediate needs. The ‘lens’ metaphor developed in the Pad++ system (Bederson and Meyer, 1998) provides a good candidate approach to this problem.

4.3 INFOCON and THREATCON

The peculiarities of cyberspace preclude strong parallels between defensive details in that domain versus (e.g.) ‘geospace’. There is, however, an obvious parallel involving own-force / own-system defensive posture. Some clear and unambiguous depiction of current ‘INFOCON’ and ‘THREATCON’ status (and perhaps even “DEFCON”) should be a canonical component of the Datawall data presentation(s). At the date of this writing, it remains unclear what the final form of USAF INFOCON protocols will be. Similarly, the optimum means for providing watch center warfighters with THREATCON and INFOCON status is an open issue. The information and display engineering for effective THREATCON / INFOCON presentation is therefore an important part of our project.

4.4 Information Pertaining to Coordination among IO Warfighters

Any one operations center is not the sole player in USAF information operations. Within USAF, each center must interact and interoperate with other organizations. Externally, the “global-level” watch center is the nexus of USAF contact with other non-USAF watch centers, both military (e.g., DISA) and non-military (e.g., FBI). The extreme speed of changes within the IO battlespace mandates measures to minimize inefficiencies in cross-unit coordination and collaboration. Further analysis and simulations will be needed to illuminate how watch center technologies can usefully promote ‘cross-agency situation awareness’—e.g., by displaying data relating to what other watch centers are doing. This could be as simple as a pop-up window showing the INFOCON status of each collaborator located elsewhere than the watch center.

4.5 Allocation of Data and Information among Watch Center Platforms

Another important issue for display planning concerns the distribution / allocation of data rather than the data itself. In the second-generation JFACC After Next testbed at Rome, the Datawall array is installed at the front of a room populated with several rows of desks, each holding multiple operator workstations. This testbed was specifically designed to allow for many operators performing individual tasks at individual workstations in addition to whatever was being done with Datawall itself. Large as it may be, the Datawall does not provide infinite display ‘real estate’. Furthermore, there may be considerable amounts of data which are specific to one or another operator’s duties, and therefore not appropriate for Datawall display to the overall watch center team.

It is likely to be a persistent issue as to which and how much data should be allocated to the large / group display, and which and how much data should be allocated for individual operators’ workstations (whatever form those workstations may take). The allocation of one or another data element / data type to one or another non-Datawall device may shift during the course of the proposed work. For example, some data initially displayed visually on the large screen may later be delivered to operators via headsets (i.e., as audio streams) or virtual reality apparatus (some years hence). It is also likely that during the projected course of Datawall work, the proportionate ‘mix’ of individual versus group display demands may shift.

In addition, there will be issues regarding the mix of common versus specific data that must be shared among the main watch center and its staff members on station in theaters of operations worldwide. The data allocation tactics appropriate to those staff members physically co-located in the main watch center do not necessarily pertain to their remotely located teammates.

4.6 Coordination among 'Big Picture' (e.g., Datawall) Users

As a large-scale interface facility in use by a watch center crew, Datawall presents issues of coordination among the people interacting with it. For example, sharing and/or turn taking protocols regarding remote laser pointers (and subsystem control protocols, in general) need to be both supported and reinforced by the specifics of the array's functionality. Unless headsets and microphones are exclusively employed, speech interaction with Datawall may require attention to turn taking to prevent background noise interference with the speech interface's operation. A common tactic for maintaining intra-team interpersonal situational awareness has been graphic presentation of data cueing individuals on (e.g.) whose turn it is and/or whether anyone 'has the conn' (e.g., a highlighted personal icon indicating whose turn it is). The necessity of addressing this issue is clear. However, a final decision on whether to implement such capabilities and the details of any such capabilities implemented will have to await further clarification of specific applications and modes of operator interaction.

In summary, the general information support requirements of the watch center will be numerous and complex. The reason we have stated these requirements so generally is that the specifics of their implementation must await and be tailored to fit the details of the relevant CONOPS, tasking, organizational structuring, training, and deployment of USAF IO units. Because research and development may well proceed in parallel with deployment, programmatic planning must be undertaken with this in mind. In the next section, we shall introduce our research program ("Cyber Warrior") and explain how it has been structured to address this situation.

5. "CYBER WARRIOR"

Advanced information portrayal and multi-sensory human-computer interfaces offer potential benefits to watch center warfighters. The Human Effectiveness Directorate of the Air Force Research Laboratory is seeking to mature and transition these technologies through the mechanism of an advanced development project*: "Cyber Warrior."* "Cyber Warrior's" objective is to demonstrate a next-generation user-centered suite of technologies to support MAJCOM and global-level DIW functions. The specific target capabilities to be developed and demonstrated include:

- **Tailored Information Management and Portrayal**: Provide the right information to the right decision-maker in the right format by tailoring information to reflect decision makers' command authority, expertise, preferences, and information needs.

- **Distributed and Collaborative Decision Support Systems and Job Performance Aids**: Support global reachback and forward deployed decision makers by designing for real-time networked operations.

- **Multi-Sensory User-System Interfaces**: Provide warfighters with information presentation and manipulation capabilities beyond those currently afforded by workstations (e.g., 3D audio, large-scale group displays, alternatives to the 'mouse').

- **Untethered Engagement with Systems**: Provide commanders the ability to operate in a natural style unrestrained by proximity to a desktop workstation.

These target capabilities are being developed so as to implement two key innovations. The first innovation pertains to the effort's products themselves—i.e., to explicitly design systems to support a distributed, collaborative team environment affording warfighters the optimized worldwide situational assessment and risk assessment capabilities required to successfully defend USAF information resources. The second innovation pertains to the process of achieving the first innovation -- i.e., applying a cognitive systems engineering approach (explicitly focusing on human information processing and decision making) to effect human-centered software support via "active user interfaces" (Brown, Santos Jr. and Banks 1999) employing a combination of intelligent agents and user models. "Cyber Warrior's" payoffs lie in maximizing crew performance through decision-optimized system design.

Our project plan delineates "Cyber Warrior" technology development approach as a recursive spiral development process with a 'cycle time' of 12 months. The recursiveness is intended to allow feed-forward of results for incremental improvement. The 12-month cycle frequency will allow Cyber Warrior to demonstrate its state-of-the-art, integrated hardware and software technologies in warfighter exercises such as JEFX. "Cyber Warrior's" end-state deliverables will include the design processes and a user-centered suite of software applications/tools and user-system interface hardware to support information operations command and control centers.

The first step toward these goals is being undertaken in "Cyber Warrior's" initial FY00/FY01 program, which will set the stage for rapid upgrading of both test bed and operational capabilities to produce and demonstrate significantly more advanced interface technologies than are currently available. It will position us to specify, design, and test even more sophisticated capabilities in an orderly progressive manner—e.g., 3-D visualization and individual operators' environments by the close of FY05; distributed collaborative virtual environments and 'untethered' operators by the close of FY10. More importantly, the FY00/FY01 program will generate a series of near-term products valuable to the ramp-up of USAF IO capabilities underway during this period, and thus contribute to meeting what we now recognize to be the most dangerous emerging threat to our national security.

The "Cyber Warrior" program has begun the process of conducting a series of field data collections in support of the cognitively based design of a future information operations watch center. The functions of the watch center are new, complex, and evolving. The elicitation, representation and validation of domain expertise are crucial to achieving "Cyber Warrior's" advanced development goals. Characteristics of an effective field data collection methodology have been identified to include:

- capable of capturing (naturalistic) decision making events
- capable of discriminating between "expert" and "novice" performance
- based on critical decision making approaches
- commercial-off-the-shelf maturity
- (semi-) automated.

In accordance with these criteria, we have selected Klein Associates' ACTA (Applied Cognitive Task Analysis) package as our primary tool for collating and processing the field data. The results will be fed forward to provide more detailed and structured analytical models for effective watch center operations. One example is the "Cyber Warrior" goal of generating specifications for the measures of outcomes, effectiveness, and performance most critical to IO functions.

6. CONCLUSIONS

The "Cyber Warrior" program has been planned with primary attention to USAF and DoD requirements for the new century. Rather than pursuing insertion of selected current technologies into emerging IO watch centers, we have 'taken the long-term view' by working from projected watch center needs toward specification of the best support technologies (whether currently deployable or not). This article's expository progression has illustrated this line of conceptual development. Our approach has been qualified with regard to the cognitive (i.e., informational) dimensions of information operations because (a) these are the critical dimensions of the mission and (b) these fall within the purview of AFRL/HE expertise. We believe Cyber "Warrior's" project plan is sound because it is grounded in careful analyses of prospective USAF and DoD missions and requirements.

7. REFERNCES

Bederson, B. & Meyer, J., *Software: Practice and Experience*, 1998 (in press).

Bolstad, C. A. & Endsley, M. R., "Shared Mental Models and Shared Displays: An Empirical Evaluation of Team Performance, *Proceedings of the Human Factors and Ergonomics Society 43rd Annual Meeting*, September 27 – October 1, 1999.

Boyd, J. R. (1987), *A Discourse on Winning and Losing*, Air University Library, Report No. MU 43947 (unpublished briefing), Maxwell Air Force Base, Alabama.

Brown, S.M., Santos Jr., E., & Banks, S.B., "Active User Interfaces for Building Decision-Theoretic Systems", In *Proceedings of the 1st Asia-Pacific Conference on Intelligent Agent Technology*, Hong Kong, 1999.

Flach, J. & Kuperman, G. G., *Victory by Design: War, Information, and Cognitive Systems Engineering*, Technical Report, AFRL-HE-WP-TR-1998-0074, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio, February 1998.

Grossman, E., "Air Force's New 'Strategic Vision' To Include Global 'Vigilance'", Inside The Pentagon, Washington DC, December 2, 1999 (page 1).

Harreld, H., "Cyberattacks spur new warning system," National Defense, March 23, 1998 (http://csel.cs.colorado.edu/~ife/l14/defense.html)

Klein, G., *Implications of the Naturalistic Decision Making Framework for Information Dominance*, Technical Report AL/CF-TR-1997—0155, Armstrong Laboratory, Wright-Patterson Air Force Base, Ohio, July 1997.

Klein, G. A., Calderwood, R., & MacGregor, D. (1989), "Critical decision method for eliciting knowledge," *IEEE Transactions on Systems, Man, and Cybernetics,* 19(3), 462-472.

Kuperman, G. G., "Cognitive Systems Engineering for Battlespace Dominance," *Proceedings of the Fourth Conference on Naturalistic Decision Making*, The Airlie Conference Center, Warrenton, Virginia, 29 - 31 May 1998.

Kuperman, G. G., "Selection of Field Data Collection Techniques," *Proceedings of the Fifth Conference on Naturalistic Decision Making*, Tammsvik Conference Center, Stockholm, Sweden, 26 – 28 May 2000.

Larsen, G. J., *Event Sequence Analysis of the Air Intelligence Agency Information Operations Center Flight Operations*, Technical Report, AFRL-HE-TR-1998-0057, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio, April 1998.

Llinas, J., Drury, C., Bialas, W. & Chen, A., *Studies and Analyses of Vulnerabilities in Aided Adversarial Decision Making*, Technical Report AFRL/HE-WP-TR-1998-0099, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio, February 1998.

MacMillan, J., Serfaty, D., Cohen, M., Freeman, J., Klein, G. & Thordsen, M., *Advanced Multimodal Watchstation Project QUICK LOOK: Critical Decisions in the AMMWS Air Dominance Scenario*, October 15, 1997

McCloskey, M. J., & Stanard, T., "A Red Team Analysis of the Electronic Battlefield: A Cognitive Approach to Understanding How Hackers Work in Groups," *Proceedings of the Human Factors and Ergonomics Society 43rd Annual Meeting*, September 27 – October 1, 1999.

National Institute of Standard and Technology (NIST), *Integration Definition for Function Modeling (IDEF0)*, Federal Information Processing Standard Publication 183, 1993 December 21. http://www.idef.com/

Pliske, R., Klinger, D., Hutton, R., Crandall, B., Knight, B., & Klein, G., *Understanding Skilled Weather Forecasting: Implications for Training and the Design of Forecasting Tools*, Contractor Report, AL/HR-CR-1997-0003, Armstrong Laboratory, Brooks Air Force Base, Texas, June 1997.

Widnall, Secretary of the Air Force S., and Chief of Staff of the Air Force Gen R. Fogleman, *Global Engagement: A Vision for the 21st Century Air Force*, 1996.

Shalikashvili , Gen J. M., Chairman of the Joint Chiefs of Staff, *Joint Vision 2010: America's Military Preparing for Tomorrow*, 1996.

Stein, G. J., *Information Warfare*, in Campen, Dearth, and Gooden (Editors), Cyberwar: Security, Strategy, and Conflict in the Information Age (Fairfax, VA: AFCEA International Press, 1996), 175-183.

Whitaker, R. D., & Kuperman, G. G., *Cognitive Engineering for Information Dominance: A Human Factors Perspective*, Technical Report, AL/CF-TR-1996-0159, Armstrong Laboratory, Wright-Patterson Air Force Base, Ohio, October 1996.

Biographies

Gilbert G. Kuperman

Mr. Gilbert G. Kuperman is assigned as Principal Mathematician in the Information Analysis and Exploitation Branch, Crew Systems Interface Division, Human Effectiveness Directorate of the Air Force Research Laboratory. He has authored more that 140 papers, reports and journal articles. He has been awarded 10 United States patents.

Scott M. Brown, Capt. USAF, Ph.D.

Captain Brown is an artificial intelligence researcher assigned to the Information Analysis and Exploitation Branch, Crew Systems Interface Division, Human Effectiveness Directorate of the Air Force Research Laboratory. He received his Ph.D. in Computer Engineering at AFIT in 1998. His current research interests include user-interface agents, interface agent development environments, expert systems, and information management systems.

Randall D. Whitaker, Ph.D.

Dr. Whitaker is a Senior Scientist with Logicon Technical Services, Inc., supporting the Information Analysis and Exploitation Branch, Crew Systems Interface Division, Human Effectiveness Directorate of the Air Force Research Laboratory. His research specialties include collaborative information technologies and human interactivity in cyberspace.